ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27006— 2008

Информационная технология Методы и средства обеспечения безопасности

ТРЕБОВАНИЯ К ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ АУДИТ И СЕРТИФИКАЦИЮ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ISO/IEC 27006:2007
Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems (IDT)

Издание официальное

БЗ 12—2008/543

Москва
Стандартинформ
2010

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 5

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 524-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27006:2007 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» (ISO/IEC 27006:2007 «Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении Е

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2010

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 1
4 Принципы . . . 2
5 Общие требования . . . 2
5.1 Юридические и договорные вопросы . . . 2
5.2 Менеджмент беспристрастности . . . 2
5.3 Обязательства и финансирование . . . 2
6 Требования к структуре . . . 2
6.1 Структура организации и высшее руководство . . . 2
6.2 Комитет по обеспечению защиты беспристрастности . . . 2
7 Требования к ресурсам . . . 3
7.1 Компетентность руководства и персонала . . . 3
7.2 Персонал, участвующий в деятельности по сертификации . . . 3
7.3 Привлечение отдельных внешних аудиторов или внешних технических экспертов . . . 5
7.4 Записи данных о персонале . . . 5
7.5 Аутсорсинг . . . 5
8 Требования к информации . . . 5
8.1 Общедоступная информация . . . 5
8.2 Документы по сертификации . . . 5
8.3 Список сертифицированных клиентов . . . 6
8.4 Ссылка на сертификацию и использование маркировки . . . 6
8.5 Конфиденциальность . . . 6
8.6 Обмен информацией между органом сертификации и его клиентами . . . 6
9 Требования к процессу . . . 6
9.1 Общие требования . . . 6
9.2 Первоначальный аудит и сертификация . . . 9
9.3 Деятельность по надзору . . . 12
9.4 Повторная сертификация . . . 13
9.5 Специальные аудиты . . . 13
9.6 Приостановка, отмена или сокращение сферы действия сертификации . . . 13
9.7 Апелляции . . . 13
9.8 Жалобы . . . 13
9.9 Документы заявителей и клиентов . . . 14
10 Требования системы менеджмента к органам сертификации . . . 14
10.1 Варианты . . . 14
10.2 Вариант 1 — Требования системы менеджмента в соответствии с ИСО 9001 . . . 14
10.3 Вариант 2 — Общие требования системы менеджмента . . . 14
Приложение А (справочное) Анализ сложности организации-клиента и аспектов, специфических для секторов торгово-промышленной деятельности . . . 15
Приложение В (справочное) Примерные области компетентности аудитора . . . 18
Приложение С (справочное) Продолжительность аудита . . . 20
Приложение D (справочное) Руководство по анализу реализованных мер управления из приложения А ИСО/МЭК 27001:2005 . . . 24
Приложение Е (обязательное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам . . . 35

Введение

ИСО/МЭК 17021 — это международный стандарт, устанавливающий критерии для органов, осуществляющих аудит и сертификацию систем менеджмента организаций. Если эти органы должны быть аккредитованы как соответствующие ИСО/МЭК 17021 с целью проведения аудита и сертификации систем менеджмента информационной безопасности (СМИБ) в соответствии с ИСО/МЭК 27001:2005, то необходимы дополнительные требования и руководства к ИСО/МЭК 17021. Они представлены в настоящем международном стандарте.

Текст настоящего международного стандарта повторяет структуру ИСО/МЭК 17021, а дополнительные требования, специфические для СМИБ, и руководство по применению ИСО/МЭК 17021 для сертификации СМИБ обозначаются аббревиатурой «ИБ».

Термин «должен» используется в этом международном стандарте для указания тех условий, которые, отражая требования ИСО/МЭК 17021 и ИСО/МЭК 27001, являются обязательными. Термин «следует» используется для обозначения условий, которые, хотя и являются руководством по применению этих требований, но предполагается, что они будут приняты органом сертификации.

Цель настоящего международного стандарта — дать возможность органам аккредитации более эффективно применять стандарты, по которым они обязаны оценивать органы сертификации. В этом контексте любое отклонение органа сертификации от руководства является исключением. Такие отклонения будут разрешены только на основе рассмотрения каждого случая в отдельности после того, как орган сертификации докажет органу аккредитации, что это исключение удовлетворяет каким-либо эквивалентным образом соответствующему пункту требований ИСО/МЭК 17021, ИСО/МЭК 27001 и настоящего международного стандарта.

Примечание — В данном международном стандарте термины «система менеджмента» и «система» используются, заменяя друг друга. Определение системы менеджмента можно найти в ИСО/МЭК 9000:2005. Систему менеджмента, использующуюся в этом международном стандарте, не следует путать с другими типами систем, такими как системы информационных технологий.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология
Методы и средства обеспечения безопасности

ТРЕБОВАНИЯ К ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ АУДИТ И СЕРТИФИКАЦИЮ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems

Дата введения — 2009—10—01

1 Область применения

Настоящий стандарт на основе стандартов ИСО/МЭК 17021 и ИСО/МЭК 27001 устанавливает требования к органам, осуществляющим аудит и сертификацию системы менеджмента информационной безопасности (СМИБ), и способствует проведению аккредитации органов сертификации.

Любой орган, осуществляющий сертификацию СМИБ, должен продемонстрировать в плане компетентности и надежности свое соответствие требованиям данного стандарта, а содержащиеся в стандарте указания дополнительно разъясняют эти требования к органу, осуществляющему сертификацию СМИБ.

Примечание — Настоящий стандарт может использоваться в качестве документа, содержащего критерии для аккредитации, экспертной оценки или других процессов аудита.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО/МЭК 17021:2006 Оценка соответствия. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента

ИСО/МЭК 27001:2005 Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ИСО/МЭК 19011:2002 Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 17021, ИСО/МЭК 27001, а также следующие термины с соответствующими определениями:

3.1 **сертификат** (certificate): Документ, выданный органом сертификации в соответствии с условиями его аккредитации и содержащий соответствующий символ или заявление об аккредитации.

3.2 **орган сертификации** (certification body): Третья сторона, оценивающая и сертифицирующая СМИБ организации-клиента на соответствие действующим стандартам СМИБ и любой дополнительной документации, требуемой в рамках этой системы.

3.3 **документ сертификации** (certification document): Документ, указывающий, что СМИБ организации-клиента соответствует стандартам СМИБ и дополнительной документации, требуемой в рамках этой системы.

Издание официальное

3.4 **маркировка** (mark): Юридически зарегистрированный товарный знак или защищенный иным образом символ, который выпускается по правилам органа аккредитации или органа сертификации, указывающий на то, что орган достаточно уверен в системах или что соответствующие продукты или субъекты отвечают требованиям определенного стандарта.

3.5 **организация** (organization): Государственная или частная компания, корпорация, фирма, предприятие, управление или учреждение или их часть, или их комбинация, имеющая собственные функции и администрацию и способная обеспечить информационную безопасность.

4 Принципы

Применяются принципы ИСО/МЭК 17021:2006, пункт 4.

5 Общие требования

5.1 Юридические и договорные вопросы

Применяются требования ИСО/МЭК 17021:2006, пункт 5.1.

5.2 Менеджмент беспристрастности

Применяются требования ИСО/МЭК 17021:2006, пункт 5.2. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

5.2.1 ИБ 5.2 Конфликты интересов

Орган сертификации может выполнять следующие обязанности, без которых он считается консультативным органом, имеющим потенциальный конфликт интересов:

a) сертификацию, включая информационные совещания, совещания по планированию, изучение документов, проведение аудита (не внутренних аудитов СМИБ или внутренних проверок безопасности) и последующую деятельность в отношении несоответствий;

b) организацию курсов обучения и участие в них в качестве преподавателя при условии, что если эти курсы связаны с менеджментом информационной безопасности, взаимосвязанными системами менеджмента или с проведением аудита, то органам сертификации необходимо ограничиваться предоставлением общей информации и рекомендациями, являющимися свободно доступным общественным достоянием, т.е. они не должны предоставлять консультации, ориентированные на конкретную компанию, что противоречит требованиям пункта c);

c) обеспечение доступности или публикацию по запросу информации, описывающей интерпретацию органом сертификации требований стандартов по сертификационному аудиту;

d) проведение мероприятий, предшествующих аудиту, имеющих целью исключительно определение готовности к сертификационному аудиту; однако подобные действия не должны приводить к предоставлению рекомендаций или консультаций, противоречащих этому пункту, и орган сертификации должен уметь подтвердить, что подобные действия не противоречат этим требованиям и не используются для обоснования возможного сокращения продолжительности сертификационного аудита;

e) проведение аудитов второй и третьей стороной в соответствии со стандартами или нормативными требованиями, кроме тех, которые являются частью области аккредитации;

f) повышение значимости сертификационных аудитов и инспекций с целью надзора, например, путем определения благоприятных возможностей для улучшений, которые становятся очевидными в процессе аудита, не рекомендуя при этом конкретных решений.

Орган сертификации должен быть независим от органа или органов (включая любых лиц), осуществляющих внутренний аудит подлежащей сертификации СМИБ организации-клиента.

5.3 Обязательства и финансирование

Применяются требования ИСО/МЭК 17021:2006, пункт 5.3.

6 Требования к структуре

6.1 Структура организации и высшее руководство

Применяются требования ИСО/МЭК 17021:2006, пункт 6.1.

6.2 Комитет по обеспечению защиты беспристрастности

Применяются требования ИСО/МЭК 17021:2006, пункт 6.2.

7 Требования к ресурсам

7.1 Компетентность руководства и персонала

Применяются требования ИСО/МЭК 17021:2006, пункт 7.1. Кроме того, применяются следующие, специфические для СМИБ, требования и руководство.

7.1.1 ИБ 7.1 Компетентность руководства

В число основных элементов обеспечения компетентности, требующихся для проведения сертификации СМИБ, входят отбор, представление специалистов, чьи навыки и общая компетентность соответствуют видам деятельности, предназначенным для аудита, и связанным с ними проблемам в области информационной безопасности, и руководство ими.

7.1.1.1 Анализ компетентности и проверка договора

Орган сертификации должен гарантировать знание им технологических и правовых вопросов, относящихся к СМИБ организации-клиента, которую он оценивает.

Орган сертификации должен обладать эффективной системой для анализа компетентности в сфере менеджмента информационной безопасности, применимой по отношению ко всем техническим областям, в которых он действует.

В отношении каждого клиента орган сертификации должен быть способен продемонстрировать, что он провел анализ необходимой компетентности (оценка навыков, соответствующих выявленным потребностям) исходя из требований каждого соответствующего сектора торгово-промышленных отношений до осуществления проверки договора. Затем орган сертификации должен осуществить проверку договора с организацией-клиентом, основываясь на результатах анализа компетентности. В частности, орган сертификации должен быть способен продемонстрировать, что он обладает компетентностью для выполнения следующих видов деятельности:

a) изучение сфер деятельности организации-клиента и связанных с ними деловых рисков;

b) определение уровня компетентности, необходимой органу сертификации для осуществления сертификации в отношении определенной деятельности, связанной с информационной безопасностью, угроз активам, уязвимостей и воздействий на организацию-клиента;

c) подтверждение наличия требуемой компетентности.

7.1.1.2 Ресурсы

Руководство органа сертификации должно располагать необходимыми процедурами и ресурсами для определения компетентности отдельных аудиторов в отношении задач, которые они должны выполнить в области сертификации, в рамках которой они действуют. Компетентность аудиторов может быть установлена на основе подтвержденного опыта и специального обучения или путем собеседования (см. также приложение В). Орган сертификации должен быть способен эффективно поддерживать связь с клиентами, которым он предоставляет услуги.

7.2 Персонал, участвующий в деятельности по сертификации

Применяются требования ИСО/МЭК 17021:2006, пункт 7.2. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

7.2.1 ИБ 7.2 Компетентность персонала органа сертификации

Органы сертификации должны иметь персонал, обладающий компетентностью в следующих вопросах:

a) выбор аудиторов СМИБ, соответствующих целям аудита, и проверка их компетентности;

b) инструктаж аудиторов СМИБ и организация необходимого обучения;

c) принятие решения о разрешении, поддержке, отмене, приостановке, продлении или сокращении сроков действия сертификации;

d) организация и ведение работ по рассмотрению апелляций и жалоб.

7.2.1.1 Обучение аудиторских групп

У органа сертификации должны быть критерии обучения аудиторских групп, обеспечивающие:

a) знание стандарта СМИБ и других соответствующих нормативных документов;

b) понимание вопросов информационной безопасности;

c) понимание оценки риска и менеджмента риска с точки зрения деятельности;

d) технические знания о деятельности, подлежащей аудиту;

e) общее знание нормативных требований, относящихся к СМИБ;

f) знание систем менеджмента;

g) понимание принципов аудита, основанных на ИСО 19011:2002;

h) знание анализа эффективности СМИБ и измерения эффективности средств контроля.

Эти требования к обучению применяются ко всем членам аудиторской группы, за исключением требований пункта (d), которые можно распределить между членами аудиторской группы.

7.2.1.1.1 При выборе аудиторской группы, которая будет назначена для конкретного сертификационного аудита, орган сертификации должен обеспечить, чтобы члены группы обладали соответствующими необходимыми навыками для каждого задания. Группа должна:

a) обладать соответствующими техническими знаниями о конкретных действиях в рамках области применения СМИБ, для которой проводится сертификация, и, если необходимо, со взаимосвязанными процедурами и их потенциальными рисками информационной безопасности (эту функцию могут выполнять технические эксперты, не являющиеся аудиторами);

b) обладать достаточным уровнем знания работы организации-клиента для проведения надежного сертификационного аудита ее СМИБ в части менеджмента аспектов, связанных с информационной безопасностью ее деятельности, продуктов и услуг;

c) обладать соответствующим знанием нормативных требований к СМИБ организации-клиента.

7.2.1.1.2 При необходимости аудиторская группа может дополняться техническими экспертами, которые должны обладать специальными знаниями в области технологии, подлежащей аудиту. Необходимо отметить, что технических экспертов нельзя использовать вместо аудиторов СМИБ, но они могут консультировать аудиторов по вопросам технической адекватности в контексте системы менеджмента, подвергающейся аудиту. Органы сертификации должны осуществлять процедуры по следующим вопросам:

a) выбор аудиторов и технических экспертов на основе их компетентности, обучения, квалификации и опыта;

b) первоначальная оценка поведения аудиторов и технических экспертов во время проведения сертификационного аудита и последующий мониторинг деятельности аудиторов и технических экспертов.

7.2.1.2 Управление процессом принятия решений

Руководство должно быть технически грамотным и способным управлять процессом принятия решений относительно разрешения, поддержки, продления, сокращения, приостановки и отмены сертификации СМИБ по требованиям ИСО/МЭК 27001.

7.2.1.3 Необходимые уровни образования, профессионального опыта, аудиторского обучения и аудиторского опыта аудиторов, проводящих аудиты системы менеджмента информационной безопасности

7.2.1.3.1 Приведенные ниже критерии должны применяться к каждому аудитору из аудиторской группы, осуществляющей аудит СМИБ. Аудитор должен:

a) иметь образование не ниже среднего;

b) иметь опыт практической работы в режиме полной занятости в области информационных технологий не менее четырех лет, из которых он не менее двух лет должен был заниматься деятельностью, связанной с информационной безопасностью;

c) успешно завершить обучение продолжительностью не менее пяти дней, программа которого включает вопросы аудита СМИБ и менеджмента аудита;

d) приобрести опыт, касающийся всего процесса оценки информационной безопасности, до принятия на себя ответственности за деятельность в качестве аудитора. Этот опыт должен быть приобретен посредством участия, как минимум, в четырех аудитах сертификации общей продолжительностью, по крайней мере, двадцать дней, включая проверку документации и анализ риска, оценку реализации и составление отчета о результатах аудита;

e) обладать достаточным современным опытом;

f) уметь рассматривать сложные операции в широкой перспективе и понимать роль отдельных подразделений в крупных организациях-клиентах;

g) поддерживать свои знания и навыки в сфере информационной безопасности и аудита на современном уровне путем постоянного повышения профессионального уровня.

Технические эксперты должны соответствовать критериям пунктов a), b), e) и f).

7.2.1.3.2 В дополнение к требованиям из пункта 7.2.1.3.1 начальники аудиторских групп должны удовлетворять следующим требованиям, которые должны быть представлены в ходе аудитов, проведенных под их руководством и наблюдением:

a) обладать знаниями и качествами, необходимыми для управления процессом сертификационного аудита;

b) иметь опыт участия в качестве аудитора, по крайней мере, в трех полных аудитах СМИБ;

c) обладать способностью эффективно общаться как в письменной, так и в устной форме.

7.3 Привлечение отдельных внешних аудиторов или внешних технических экспертов

Применяются требования ИСО/МЭК 17021:2006, пункт 7.3. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

7.3.1 ИБ 7.3 Привлечение внешних аудиторов или внешних технических экспертов в качестве членов аудиторской группы

При привлечении внешних аудиторов или внешних технических экспертов в качестве членов аудиторской группы орган сертификации должен гарантировать, что они компетентны, соответствуют применимым к ним положениям настоящего стандарта и не участвуют ни напрямую, ни через своего работодателя в проектировании, внедрении или обслуживании СМИБ или связанной с ней системой (системами) менеджмента, поскольку это могло бы влиять на их беспристрастность.

7.3.1.1 Привлечение технических экспертов

Членами аудиторской группы могут быть технические эксперты со специальными знаниями, касающимися процесса и вопросов, связанных с информационной безопасностью и безопасностью процесса, и законодательства, затрагивающего интересы организации-клиента, но не удовлетворяющие всем критериям пункта 7.2. Технические эксперты должны работать под наблюдением аудитора.

7.4 Записи данных о персонале

Применяются требования ИСО/МЭК 17021:2006, пункт 7.4.

7.5 Аутсорсинг

Применяются требования ИСО/МЭК 17021:2006, пункт 7.5.

8 Требования к информации

8.1 Общедоступная информация

Применяются требования ИСО/МЭК 17021:2006, пункт 8.1. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

8.1.1 ИБ 8.1 Процедуры разрешения, поддержания, продления, сокращения, приостановления и отказа в сертификации

Орган сертификации должен требовать от организации-клиента наличия документированной и внедренной СМИБ, которая соответствует ИСО/МЭК 27001 и другим документам, необходимым для сертификации.

У органа сертификации должны быть документально подтвержденные процедуры для следующего:

a) первичного сертификационного аудита СМИБ организации-клиента в соответствии с положениями ИСО 19011, ИСО/МЭК 17021 и другими соответствующими документами;

b) надзорных и повторных сертификационных аудитов СМИБ организации-клиента в соответствии с ИСО 19011 и ИСО/МЭК 17021, проводимых периодически на предмет проверки непрерывного соответствия определенным требованиям, а также для подтверждения и регистрации, что организация-клиент своевременно предпринимает корректирующие действия по исправлению всех несоответствий.

8.2 Документы по сертификации

Применяются требования ИСО/МЭК 17021:2006, пункт 8.2. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

8.2.1 ИБ 8.2 Документы по сертификации СМИБ

Орган сертификации должен предоставить каждой из своих организаций-клиентов, чья СМИБ сертифицирована, документы по сертификации, такие как письмо или сертификат, подписанный уполномоченным должностным лицом. Для организации-клиента и каждой из ее сертифицированных информационных систем эти документы должны определять область действия сертификации и соответствовать стандарту ИСО/МЭК 27001 по СМИБ, по которому эта СМИБ сертифицирована. Кроме того, в сертификате должна быть ссылка на определенную версию Положения о применимости.

8.3 Список сертифицированных клиентов

Применяются требования ИСО/МЭК 17021:2006, пункт 8.3.

8.4 Ссылка на сертификацию и использование маркировки

Применяются требования ИСО/МЭК 17021:2006, пункт 8.4. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

8.4.1 ИБ 8.4 Контроль за маркировками сертификации

Орган сертификации должен осуществлять надлежащий контроль за правом собственности, использованием и демонстрацией своих сертификационных знаков СМИБ. Если орган сертификации дает право использовать знак для обозначения сертификации СМИБ, то он должен быть уверен, что организация-клиент использует специальный знак в соответствии с письменным разрешением, полученным от органа сертификации. Орган сертификации не должен позволять организации-клиенту использовать этот знак на продукте таким способом, что он может интерпретироваться в качестве обозначения соответствия продукта.

8.5 Конфиденциальность

Применяются требования ИСО/МЭК 17021:2006, пункт 8.5. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

8.5.1 ИБ 8.5 Доступ к документам организации

Перед проведением аудита орган сертификации должен сделать запрос организации-клиенту о наличии документов о СМИБ, которые не могут быть предоставлены для проверки аудиторской группе, так как они содержат конфиденциальную или секретную информацию. Орган сертификации должен определить, может ли быть адекватным проведение аудита СМИБ при отсутствии этих документов. Если орган сертификации приходит к выводу, что невозможно провести аудит СМИБ адекватно без проверки определенных конфиденциальных или секретных документов, он должен предупредить организацию-клиента, что сертификационный аудит не может быть проведен до тех пор, пока не будет обеспечен доступ к этим документам.

8.6 Обмен информацией между органом сертификации и его клиентами

Применяются требования ИСО/МЭК 17021:2006, пункт 8.6.

9 Требования к процессу

9.1 Общие требования

Применяются требования ИСО/МЭК 17021:2006, пункт 9.1. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

9.1.1 ИБ 9.1.1 Общие требования к аудиту СМИБ

9.1.1.1 Критерии сертификационного аудита

Аудит СМИБ организации-клиента должен осуществляться на основе критериев, содержащихся в стандарте ИСО/МЭК 27001 по СМИБ, а также в других документах, необходимых для проведения сертификации конкретных выполняемых функций. Если требуется разъяснение в отношении применения этих документов к конкретной программе сертификации, то подобное разъяснение должно даваться соответствующей независимой комиссией или лицами, обладающими необходимой технической компетентностью, и публиковаться органом по сертификации.

9.1.1.2 Политика и процедуры

Документация органа сертификации должна включать политику и процедуры осуществления процесса сертификации, включая проверки применения документов, использованных при сертификации систем СМИБ, а также процедуры проведения аудита и сертификации СМИБ организации-клиента.

9.1.1.3 Аудиторская группа

Аудиторская группа должна официально назначаться и обеспечиваться соответствующими рабочими документами. План и дата аудита должны быть согласованы с организацией-клиентом. Полномочия, данные аудиторской группе, должны быть четко определены, доведены до организации-клиента и должны обязывать аудиторскую группу проверять структуру, политику и процедуры организации-клиента, подтверждать их [структуры, политику и процедуры] соответствие всем требованиям, относящимся к области действия сертификации, а также, что указанные процедуры выполняются и можно быть уверенным в эффективности СМИБ организации-клиента.

9.1.2 ИБ 9.1.2 Область действия сертификации

Аудиторская группа должна проверить СМИБ организации-клиента, входящую в заданную область действия, на соответствие всем применяемым требованиям сертификации. Орган сертификации должен обеспечить четкое определение области действия и границы СМИБ организации-клиента на основе характеристик бизнеса, организации, ее местоположения, активов и технологии. Орган сертификации должен подтвердить, что в области действия СМИБ организации-клиенты выполняют требования, изложенные в ИСО/МЭК 27001:2005, пункт 1.2.

Органы сертификации должны обеспечить, чтобы проводимая организациями-клиентами оценка риска информационной безопасности и обработка риска надлежащим образом отражали их деятельность и распространялись до границ их сферы деятельности, как определено в стандарте ИСО/МЭК 27001 по СМИБ. Органы сертификации должны подтвердить, что все это отражено в области действия их СМИБ и в Положении о применимости организаций-клиентов.

Органы сертификации должны обеспечить, чтобы взаимодействие с услугами или видами деятельности, которые не полностью включены в сферу действия СМИБ, было учтено в сертифицируемой СМИБ и включено в оценку риска информационной безопасности организации-клиента. Примером подобной ситуации является совместное использование различных средств с другими организациями (например, системы ИТ, базы данных и системы телекоммуникации).

9.1.3 ИБ 9.1.3 Время аудита

Органы сертификации должны предоставлять аудиторам достаточное время для осуществления всех действий, связанных с первоначальным аудитом, надзорным или аудитом повторной сертификации. Время должно рассчитываться на основе таких факторов, как:

a) масштаб области действия СМИБ (например, количество используемых информационных систем, количество сотрудников);

b) сложность СМИБ (например, критичность информационных систем, ситуация с рисками СМИБ), см. также приложение А;

c) вид(ы) деятельности, осуществляемой в рамках области действия СМИБ;

d) уровень и разнообразие технологии, использованной при внедрении различных компонентов СМИБ (таких, как внедренные средства контроля, управление документацией и/или процессами, корректирующие/превентивные действия и т.д.);

e) количество объектов организации-клиента;

f) ранее продемонстрированное функционирование СМИБ;

g) объем аутсорсинга и соглашений с третьими сторонами, использованных в рамках СМИБ;

h) стандарты и нормативные требования, применяющиеся к сертификации.

В приложении С представлено руководство по продолжительности аудита. Орган сертификации должен быть готов обосновать продолжительность времени, затраченного на первоначальный аудит, надзорные аудиты или аудит повторной сертификации.

9.1.4 ИБ 9.1.4 Множественные объекты (площадки)

9.1.4.1 Решения по выборке объектов в области сертификации СМИБ являются более сложными, чем те же самые решения в системах менеджмента качества. Там, где организация-клиент имеет количество объектов сертификации, удовлетворяющее критериям от a) до c), приведенным ниже, органы сертификации могут использовать основанный на выборке подход к сертификационному аудиту многочисленных объектов:

a) все объекты работают в рамках одной и той же СМИБ, которая управляется централизованно, проверяется и подлежит проверке центральным руководством;

b) все объекты включаются в программу внутреннего аудита СМИБ организации-клиента;

c) все объекты включаются в программу проверки СМИБ руководством организации-клиента.

9.1.4.2 Орган сертификации, желающий использовать подход, основанный на выборке, должен выполнять процедуры, обеспечивающие следующее:

a) первоначальная проверка договора выявляет в максимально возможной степени разницу между объектами с целью определения адекватного объема выборки;

b) орган сертификации осуществил выборку представительного числа объектов с учетом следующего:

1) результатов внутренних аудитов главного офиса и объектов;

2) результатов анализа, проведенного руководством;

3) различий в размерах объектов;

4) различий в бизнес-целях объектов;

5) сложности СМИБ;

6) сложности информационных систем в различных объектах;

7) различий в рабочих навыках;

8) различий в предпринятых мерах;

9) потенциального взаимодействия с критическими информационными системами или информационными системами обработки информации ограниченного доступа;

10) любых отличающихся юридических требований;

c) представительный образец выбирается на всех объектах в сфере действия СМИБ организации-клиента; этот выбор должен основываться на субъективном выборе для отражения факторов, представленных в пункте b), а также элемента случайности;

d) каждый включенный в СМИБ объект, который подвергается значительным рискам, проверяется органом сертификации до проведения сертификации;

e) программа надзора, разработанная на основе вышеизложенных требований, охватывает за соответствующий период времени все объекты организации-клиента или объекты, входящие в область действия сертификации СМИБ;

f) при выявлении несоответствия в главном офисе или в одном из объектов применяются корректирующие действия по отношению к главному офису и всем сертифицируемым объектам.

Аудит, описанный в ИБ 9.1.5, должен учитывать действия главного офиса организации-клиента, чтобы гарантировать, что единая СМИБ охватывает все объекты (площадки) и обеспечивает центральное управление на оперативном уровне. Аудит должен учитывать все вышеописанные требования.

9.1.5 ИБ 9.1.5 Методология аудита

Орган сертификации должен иметь процедуры, позволяющие требовать от организации-клиента способности продемонстрировать, что внутренние аудиты СМИБ спланированы, а программа и процедуры их проведения являются действующими.

Процедуры органа сертификации не должны предполагать особого способа реализации СМИБ или особого формата для документации и записей. Процедуры сертификации должны концентрироваться на установлении того, что СМИБ организации-клиента удовлетворяет требованиям стандарта ИСО/МЭК 27001, а также политике и целям организации-клиента.

План аудита должен определять методы аудита с применением сетевых технологий, которые будут использоваться при необходимости во время аудита.

Примечание — Методы аудита с применением сетевых технологий могут включать, например, телеконференции, Интернет-совещания, интерактивную связь на базе Интернет-технологий и удаленный электронный доступ к документации СМИБ и/или процессам СМИБ. Целью применения этих методов должно быть повышение эффективности и продуктивности аудита, а также поддержание целостности процесса аудита.

9.1.6 ИБ 9.1.6 Отчет по сертификационному аудиту

9.1.6.1 Орган сертификации может использовать различные процедуры, связанные с составлением отчетов, которые соответствуют его потребностям, но эти процедуры, как минимум, должны обеспечить следующее:

a) до того, как аудиторская группа покинет территорию организации-клиента, проводится встреча аудиторской группы и руководства организации-клиента, в ходе которой аудиторская группа:

1) в письменной или устной форме сообщает о соответствии СМИБ организации-клиента определенным требованиям сертификации;

2) предоставляет возможность представителям организации-клиента задавать вопросы по поводу сделанных выводов и оснований для них;

b) представляет в орган сертификации отчет о результатах аудита в отношении соответствия СМИБ организации-клиента всем требованиям сертификации.

9.1.6.2 В отчете о результатах аудита должна быть представлена следующая информация:

a) причина аудита, включая краткое изложение анализа документов;

b) причина сертификационного аудита по анализу степени риска информационной безопасности организации-клиента;

c) общее время, затраченное на аудит, и подробное описание времени, затраченного на анализ документов, оценку анализа рисков, аудит на местах и составление отчетов о результатах аудита;

d) вопросы аудита, основная причина их выбора и примененная методология.

9.1.6.3 Отчет о результатах аудита, представленный органу сертификации, должен быть достаточно подробным для упрощения принятия решения о сертификации и его поддержки и должен содержать:

a) области, включенные в аудит (например, требования сертификации и проверенные объекты), включая значимые контрольные записи и использованные методологии аудита (см. ИБ 9.1.5);

b) наблюдения как положительного (например, заслуживающие внимания особенности), так и отрицательного (например, потенциальные несоответствия) характера;

c) подробности выявленных несоответствий, подтвержденные объективными данными, и ссылку этих несоответствий на соответствующие требования стандарта ИСО/МЭК 27001 по СМИБ или другие документы, требуемые для сертификации;

d) замечания о соответствии СМИБ организации-клиента требованиям сертификации с четким заявлением о несоответствии, ссылку на версию Положения о применимости и в случаях, где это уместно, любое полезное сравнение с результатами предыдущих сертификационных аудитов организации-клиента.

Составной частью отчета о результатах аудита могут быть заполненные опросные листы, перечни контрольных вопросов, результаты наблюдения, журналы регистрации или замечания аудитора. В случае использования соответствующих методов эти документы должны подаваться в орган сертификации в качестве свидетельства для поддержки решения о сертификации. Информацию о выборках, оцененных во время аудита, следует включить в отчет о результатах аудита или в другую документацию по сертификации.

В отчете должна рассматриваться правильность внутренней структуры и процедур, принятых организацией-клиентом для обеспечения доверия к СМИБ.

В дополнение к требованиям, предъявляемым к составлению отчетов ИСО/МЭК 17021:2006, пункт 9.1.10, отчет должен содержать:

- степень доверия к внутренним аудитам СМИБ и проверкам со стороны руководства;
- краткое изложение самых важных наблюдений как положительного, так и отрицательного характера, касающихся внедрения и результативности СМИБ;
- рекомендацию аудиторской группы в отношении того, следует ли сертифицировать СМИБ организации-клиента, с информацией для обоснования этой рекомендации.

9.2 Первоначальный аудит и сертификация

Применяются требования ИСО/МЭК 17021:2006, пункт 9.2. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

9.2.1 ИБ 9.2.1 Компетентность аудиторской группы

Приведенные ниже требования применяются к сертификационной оценке в дополнение к требованиям, перечисленным в пункте 7.2. Для действий по надзору применяются только те требования, которые имеют отношение к запланированной деятельности по надзору.

Ко всей аудиторской группе применяются следующие требования:

a) в каждой из рассмотренных областей, по крайне мере, один член аудиторской группы должен удовлетворять критериям органа сертификации, чтобы взять на себя ответственность в группе за:

1) руководство группой;

2) системы и процессы менеджмента, применимые в СМИБ;

3) знание законодательных и нормативных требований в отдельной области информационной безопасности;

4) идентификацию угроз информационной безопасности и тенденций инцидентов;

5) идентификацию уязвимостей организации-клиента и понимание вероятности их использования, влияния, уменьшения и контроля;

6) знание средств контроля СМИБ и их реализации;

7) знание анализа результативности СМИБ и средств контроля;

8) взаимосвязанные и/или соответствующие стандарты СМИБ, лучший практический опыт в промышленности, политики и процедур безопасности;

9) знание методов обработки инцидентов и обеспечения непрерывности бизнеса;

10) знание материальных и нематериальных информационных активов и анализ влияния;

11) знание современной технологии, где безопасность может быть уместной или может представлять проблему;

12) знание процессов и методов менеджмента рисков;

b) аудиторская группа должна быть компетентной для отслеживания указаний на инциденты безопасности в СМИБ организации-клиента к соответствующим элементам СМИБ;

c) аудиторская группа должна обладать соответствующим опытом работы и применять вышеуказанные пункты на практике (это не значит, что аудитор должен быть опытным во всех областях информационной безопасности, но в целом аудиторская группа должна иметь достаточные знания и опыт, чтобы охватить всю область действия проверяемой СМИБ).

Аудиторская группа может состоять из одного человека при условии, что он удовлетворяет всем вышеизложенным критериям пункта a).

9.2.1.1 ИБ 9.2.1.1 Демонстрация компетентности аудиторов

Аудиторы должны быть способны доказать свои знания и опыт, как указано выше, например посредством:

a) общепризнанных квалификаций по СМИБ;

b) регистрации в качестве аудитора;

c) пройденных курсов подготовки по СМИБ;

d) последних документов, подтверждающих факт непрерывного повышения квалификации;

e) практической демонстрации проведения аудита реальных систем клиента в присутствии других аудиторов.

9.2.2 ИБ 9.2.2 Общая подготовка к первоначальному аудиту

Орган сертификации должен потребовать от организации-клиента сделать все необходимые приготовления к проведению сертификационного аудита, включая приготовления для изучения документации и доступ ко всем областям, документам (включая отчеты о внутреннем аудите и отчеты о независимых проверках информационной безопасности) и персоналу с целью сертификационного аудита, аудита повторной сертификации и удовлетворения жалоб.

До проведения сертификационного аудита на месте организация-клиент должна предоставить следующую информацию:

a) общую информацию, касающуюся СМИБ и осуществляемых ею действий;

b) копию документации СМИБ, требуемую по ИСО/МЭК 27001:2005, пункт 4.3.1.

9.2.3 ИБ 9.2.3 Первоначальный сертификационный аудит

9.2.3.1 ИБ 9.2.3.1 Первый этап аудита

На этом этапе аудита орган сертификации должен получить документацию по проектированию СМИБ, включая документацию, требуемую по ИСО/МЭК 27001:2005, пункт 4.3.1.

Цель первого этапа аудита — обеспечить концентрацию на планировании аудита второго этапа путем ознакомления со СМИБ организации-клиента в контексте ее политики и целей и, в особенности, состояния готовности организации-клиента к аудиту.

Первый этап аудита включает проверку документации (но не должен ограничиваться ею). Орган сертификации должен договориться с организацией-клиентом о месте и времени проведения проверки документов. В любом случае проверка документов должна быть завершена до начала второго этапа аудита.

Результаты первого этапа аудита должны быть задокументированы в письменном отчете. Орган сертификации должен проанализировать отчет первого этапа аудита до вынесения решения о проведении второго этапа аудита и для выбора членов аудиторской группы с необходимым уровнем компетентности для проведения второго этапа.

Орган сертификации должен поставить в известность организацию-клиента о дополнительной информации и документах, которые могут потребоваться для тщательного изучения во время второго этапа аудита.

9.2.3.2 ИБ 9.2.3.2 Второй этап аудита

9.2.3.2.1 Второй этап аудита всегда проводится на объектах организации-клиента. На основе полученных данных, отраженных в отчете о результатах первого этапа аудита, орган сертификации намечает план проведения второго этапа аудита. Целями второго этапа аудита являются:

a) подтверждение, что организация-клиент придерживается собственных политики, целей и процедур;

b) подтверждение соответствия СМИБ всем требованиям стандарта ИСО/МЭК 27001:2005 и целям политики организации-клиента.

9.2.3.2.2 Для осуществления этого аудит должен быть сосредоточен на следующем:

a) оценке рисков информационной безопасности и на том, дают ли эти оценки сопоставимые и воспроизводимые результаты;

b) требованиях к документации, перечисленных в ИСО/МЭК 27001:2005, пункт 4.3.1;

c) выборе целей контроля и средств контроля, основанных на оценке риска и процессах обработки риска;

d) анализе результативности СМИБ и измерениях результативности средств контроля информационной безопасности, составлении отчетов и проведении анализа в отношении целей СМИБ;

e) внутренних аудитах СМИБ и анализе со стороны руководства;

f) ответственности руководства за политику информационной безопасности;

g) соответствии между выбранными и внедренными средствами контроля, заявлении о применимости и результатах оценки степени риска, процессе обработки риска, а также политики и целях СМИБ;

h) введении в действие средств контроля (см. приложение D), принимая во внимание измерения результативности средств контроля организации-клиента [см. d)], чтобы определить, реализуются ли средства контроля и эффективны ли они для достижения намеченных целей;

i) программах, процессах, процедурах, записях, внутренних аудитах и анализах эффективности СМИБ с целью обеспечения их прослеживаемости до решений менеджмента, политики и целей СМИБ.

9.2.3.3 ИБ 9.2.3.3 Особые элементы аудита СМИБ

Функцией органа сертификации является установление последовательности для организации-клиента в создании и поддержании процедур по идентификации, изучению и оценке угроз активам, связанным с информационной безопасностью, уязвимостью и воздействием на организацию-клиента. Органы сертификации должны:

a) требовать от организации-клиента свидетельства, что анализ угроз, связанных с информационной безопасностью, является значимым и соответствующим работе организации-клиента;

Примечание — Организация-клиент отвечает за определение критериев, по которым риски организации-клиента, связанные с информационной безопасностью, идентифицируются как значительные, и за разработку процедуры (процедур), необходимой для осуществления этого определения.

b) установить, согласуются ли процедуры организации-клиента по идентификации, изучению и оценке угроз, связанных с информационной безопасностью активов, уязвимости и воздействий, и результаты их применения с политикой, целями и планами организации-клиента.

Орган сертификации должен также установить, являются ли процедуры, используемые в анализе значимости, надежными и надлежащим образом реализованными. Если угроза активам, связанная с информационной безопасностью, уязвимость или воздействие на организацию-клиента идентифицированы как значимые, их менеджмент должен осуществляться в рамках СМИБ.

9.2.3.3.1 Правовое и нормативное соответствие

Поддержание и оценка выполнения правовых и нормативных норм являются обязанностью организации-клиента. Орган сертификации должен ограничиваться проверками и выборками для создания доверия к тому, что СМИБ функционирует в данном направлении. Орган сертификации должен подтверждать наличие у организации-клиента системы менеджмента для установления правового и нормативного соответствия, приемлемого для рисков информационной безопасности и воздействий на нее.

9.2.3.3.2 Интеграция документации системы менеджмента информационной безопасности с документацией других систем менеджмента

Организация-клиент может комбинировать документацию СМИБ с документацией других систем менеджмента (таких, как система менеджмента качества, охраны труда, экологического менеджмента), если СМИБ может быть четко идентифицирована вместе с соответствующими средствами других систем.

9.2.3.3.3 Объединение аудитов системы менеджмента

Орган сертификации может предложить сертификацию другой системы менеджмента, связанной с сертификацией СМИБ, или сертификацию только СМИБ.

Аудит СМИБ может объединяться с аудитами других систем менеджмента. Это объединение возможно, если аудиты удовлетворяют всем требованиям по сертификации СМИБ. Все элементы, значимые для СМИБ, должны быть четко выраженными и быть легко идентифицируемыми в отчетах о результатах аудитов. Объединение аудитов не должно отрицательно влиять на качество аудита СМИБ.

Примечание — ИСО 19011 предоставляет руководство по проведению совместных аудитов систем менеджмента.

9.2.4 ИБ 9.2.4 Информация для разрешения первоначальной сертификации

Для принятия решения о сертификации орган сертификации должен затребовать подробные отчеты, предоставляющие достаточную информацию для принятия этого решения. На разных этапах процесса сертификационного аудита органу сертификации требуются отчеты аудиторских групп. В сочетании с информацией, хранящейся в файле, эти отчеты должны содержать, по крайней мере, информацию, требуемую в ИБ 9.1.6.

9.2.5 ИБ 9.2.5 Решение о сертификации

Субъект, который может быть физическим лицом, принимающий решение о разрешении/отмене сертификации в рамках органа сертификации, должен обладать достаточным уровнем знаний и опыта во всех областях для оценки процедур аудита и рекомендаций аудиторской группы.

Решение о сертификации СМИБ организации-клиента должно приниматься органом сертификации на основе информации, собранной в процессе сертификации, и любой другой информации, относящейся к делу. Лица, принимающие решение о сертификации, не должны участвовать в аудите. Это решение должно основываться на полученных данных и рекомендациях по сертификации аудиторской группы, представленных в ее отчете о результатах сертификационного аудита (см. ИБ 9.1.6), и на любой другой релевантной информации, доступной органу сертификации.

Субъекту, принимающему решение о разрешении сертификации, обычно не следует опровергать отрицательную рекомендацию аудиторской группы. В подобной ситуации орган сертификации должен официально оформить и дать основание для решения об опровержении рекомендации.

По вопросу вынесения решения о сертификации в ИСО/МЭК 17021:2006 не упоминается о конкретном периоде времени, в течение которого должны происходить, по меньшей мере, один полный внутренний аудит СМИБ и одна проверка менеджмента организации-клиента. Этот период может устанавливаться органом сертификации. Независимо от того, принял ли орган сертификации решение об определении минимальной периодичности аудитов, им должны быть предприняты меры для обеспечения результативности анализа со стороны руководства организации-клиента и процессов внутреннего аудита СМИБ организации-клиента.

Сертификация не должна быть разрешена организации-клиенту до тех пор, пока не будет убедительного свидетельства, что мероприятия по анализу менеджмента и внутренним аудитам СМИБ были реализованы, являются эффективными и будут поддерживаться.

9.3 Деятельность по надзору

Применяются требования ИСО/МЭК 17021:2006, пункт 9.3. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

9.3.1 ИБ 9.3 Аудиты надзора

9.3.1.1 Процедуры аудита надзора должны согласовываться с процедурами, относящимися к сертификационному аудиту СМИБ организации-клиента, как определено в настоящем стандарте.

Целью надзора является подтверждение продолжения реализации утвержденной СМИБ, рассмотрение предпосылок для изменений в этой системе, инициированных в результате изменений в работе организации-клиента, и подтверждение постоянного соответствия требованиям сертификации. Программы надзора обычно должны включать:

a) элементы поддержки функционирования системы, которыми являются внутренний аудит СМИБ, анализ со стороны руководства, а также предупредительные и корректирующие действия;

b) информацию, поступающую от внешних сторон, как это требуется стандартом ИСО/МЭК 27001 и другими документами, необходимыми для сертификации;

c) изменения в документально оформленной системе;

d) области, подлежащие изменению;

e) элементы, выбранные из ИСО/МЭК 27001;

f) при необходимости другие выбранные области.

9.3.1.2 При надзоре со стороны органа сертификации подлежат анализу, как минимум, следующие факторы:

a) результативность СМИБ в отношении достижения целей политики информационной безопасности организации-клиента;

b) функционирование процедур периодической оценки и проверки соответствия правовым и нормативным требованиям, связанным с информационной безопасностью;

c) меры, принятые в отношении несоответствий, выявленных во время последнего аудита.

9.3.1.3 Надзор, осуществляемый органом сертификации, должен по меньшей мере выполняться в соответствии с пунктами, предусмотренными ИСО/МЭК 17021. При этом учитывается следующее:

a) орган сертификации должен быть способен адаптировать свою программу надзора к проблемам информационной безопасности, связанным с угрозами активам, уязвимостями и воздействиями на организацию-клиента, и обосновать эту программу;

b) программа надзора органа сертификации должна определяться органом сертификации. Конкретные даты инспекций могут согласовываться с сертифицируемой организацией-клиентом;

c) аудиты надзора могут объединяться с аудитами других систем менеджмента. В отчетах должны четко указываться аспекты, значимые для каждой системы менеджмента;

d) орган сертификации требуется для осуществления надзора за надлежащим использованием сертификата.

Во время аудитов надзора органы сертификации должны проверять записи обращений и жалоб, представленных заранее на рассмотрение органу сертификации, и в случаях обнаружения какого-либо несоответствия или невыполнения требований сертификации, записи об исследовании организацией-клиентом собственной СМИБ и процедур, а также принятии соответствующих корректирующих мер.

Отчет по надзору должен содержать в себе, в частности, информацию об устранении обнаруженных ранее несоответствий. Отчеты, полученные в результате надзора, должны собираться, чтобы в совокупности удовлетворять требованию пункта a).

9.4 Повторная сертификация

Применяются требования ИСО/МЭК 17021:2006, пункт 9.4. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

9.4.1 ИБ 9.4 Аудиты повторной сертификации

Как изложено в настоящем стандарте, процедуры аудитов повторной сертификации должны согласовываться с процедурами, относящимися к сертификационному аудиту СМИБ организации-клиента.

Органы сертификации должны иметь строго определенные процедуры, утверждающие обстоятельства и условия, при которых поддерживается сертификация. Если во время надзора или повторных сертификационных аудитов выявляются несоответствия, то они должны эффективным образом корректироваться в оговоренное органом сертификации время. Если коррекция не была проведена в согласованный срок, область действия сертификации должна быть сокращена, действие сертификата должно быть приостановлено или он должен быть отменен. Период времени, необходимый для устранения несоответствия, должен соответствовать его серьезности и риску доверия к продуктам и услугам организации-клиента.

9.5 Специальные аудиты

Применяются требования ИСО/МЭК 17021:2006, пункт 9.5. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

9.5.1 ИБ 9.5 Особые случаи

Действия по надзору должны проводиться по специальному положению в случае осуществления организацией-клиентом с сертифицированной СМИБ существенной модификации своей системы или внесения изменений, которые могут затрагивать основу ее сертификации.

9.6 Приостановка, отмена или сокращение сферы действия сертификации

Применяются требования ИСО/МЭК 17021:2006, пункт 9.6.

9.7 Апелляции

Применяются требования ИСО/МЭК 17021:2006, пункт 9.7.

9.8 Жалобы

Применяются требования ИСО/МЭК 17021:2006, пункт 9.8. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

9.8.1 ИБ 9.8 Жалобы

Жалобы являются источником информации о возможном несоответствии. Орган сертификации должен потребовать от сертифицированной организации-клиента, чтобы при получении жалобы сертифицированная организация-клиент установила и, при необходимости, сообщила причину жалобы, включая любые предопределяющие (или предрасполагающие) факторы в рамках СМИБ организации-клиента.

Органу сертификации следует самому убедиться в том, что организация-клиент использует подобные исследования для разработки корректирующих действий, в которые следует включать меры по:

a) уведомлению соответствующих органов, если это требуется по положению;

b) восстановлению соответствия;

c) предотвращению повторения;

d) оценке и смягчению любых неблагоприятных инцидентов информационной безопасности и связанных с ними воздействий;

e) обеспечению удовлетворительного взаимодействия с другими компонентами СМИБ;

f) оценке результативности принятых исправительных/корректирующих мер.

Орган сертификации должен требовать от каждой организации-клиента, чья СМИБ сертифицируется, делать доступными по его запросу записи обо всех жалобах и корректирующих мерах по их устранению, предпринятых в соответствии с требованиями ИСО/МЭК 27001:2005.

9.9 Документы заявителей и клиентов

Применяются требования ИСО/МЭК 17021:2006, пункт 9.9.

10 Требования системы менеджмента к органам сертификации

10.1 Варианты

Применяются требования ИСО/МЭК 17021:2006, пункт 10.1.

10.2 Вариант 1 — Требования системы менеджмента в соответствии с ИСО 9001

Применяются требования ИСО/МЭК 17021:2006, пункт 10.2.

10.3 Вариант 2 — Общие требования системы менеджмента

Применяются требования ИСО/МЭК 17021:2006, пункт 10.3. Кроме того, применяются следующие, специфические для СМИБ, требования и положения.

10.3.1 ИБ Внедрение системы менеджмента информационной безопасности

Рекомендуется, чтобы органы сертификации внедряли СМИБ в соответствии с ИСО/МЭК 27001:2005.

Приложение А
(справочное)

Анализ сложности организации-клиента и аспектов, специфических для секторов торгово-промышленной деятельности

А.1 Потенциал риска организации-клиента

При определении времени аудита и компетентности аудитора должна учитываться сложность СМИБ. Данное приложение является примером анализа организации-клиента.

Категория сложности, установленная для СМИБ, может использоваться для определения следующего:

a) требования к компетентности аудиторов для аудита СМИБ (пример которых дан в приложении В);

b) требования ко времени аудита СМИБ (пример которых дан в приложении С).

Таблица А.1 является общим перечнем возможных факторов, рассматриваемых при определении сложности СМИБ. Может возникнуть необходимость адаптации данной таблицы к конкретным обстоятельствам или включения специальных факторов.

Таблица А.1 — Критерии сложности области действия системы менеджмента информационной безопасности

Фактор сложности	Категория			Значимость
	высокая	средняя	низкая	
Количество сотрудников + штат подрядчиков	≥ 1000	≥ 200	< 200	Шкала реализации СМИБ Административная информационная система Системы, связанные с управлением производством Системы, связанные с продажей/распространением/общим обслуживанием Информационные технологии/Информационные услуги и связанные с ними системы Системы, связанные со строительством/судостроением/машиностроением
Количество пользователей	≥ 1000000	≥ 200000	< 200000	Финансовые системы Правительственные, учебные, медициские/больничные системы
Количество объектов	≥ 5	≥ 2	1	Шкала реализации СМИБ Физическая безопасность и безопасность окружающей среды (ИСО/МЭК 27001:2005, А.9)
Количество серверов	≥ 100	≥ 10	< 10	Шкала реализации СМИБ Физическая безопасность и безопасность окружающей среды (А.9) Управление доступом (ИСО/МЭК 27001:2005, А.11) Телекоммуникации и управление работой (ИСО/МЭК 27001:2005, А.10)
Количество рабочих станций + ПК + портативных компьютеров	≥ 300	≥ 50	< 50	Контроль доступа (ИСО/МЭК 27001:2005, А.11)
Количество персонала, занимающегося разработкой приложений и техническим обслуживанием	≥ 100	≥ 20	< 20	Приобретение, разработка и обслуживание информационных систем (ИСО/МЭК 27001:2005, А.12)

Окончание таблицы А.1

Фактор сложности	Категория			Значимость
	высокая	средняя	низкая	
Сетевая и криптографическая технология (ИСО/МЭК 27001:2005, А.9)	Внешние/ Интернет соединения с требованиями шифрования/ цифровой подписи/инфраструктуры открытых ключей	Внешние/ Интернет соединения с использованием шифрования во встроенной стандартной аппаратуре и без требований цифровой подписи/инфраструктуры открытых ключей	Внешние/ Интернет соединения без требований шифрования/ цифровой подписи/ инфраструктуры открытых ключей	Телекоммуникации и управление работой (ИСО/МЭК 27001:2005, А.10) Контроль доступа (ИСО/МЭК 27001:2005, А.11)
Значимость юридического соответствия	Несоответствие ведет к возможному судебному преследованию	Несоответствие ведет к значительным финансовым штрафам или нанесению ущерба нематериальным активам	Несоответствие ведет к незначительным финансовым штрафам или нанесению ущерба нематериальным активам	Законы и руководящие документы (ИСО/МЭК 27001:2005, А.15)
Применимость конкретного для сектора риска (см. в А.2 *примеры специфических для сектора категорий риска информационной безопасности)*	Применяются специфические для сектора законы и положения	Не применяются специфические для сектора закон и положение, но применяется значительный конкретный для сектора риск	Не применяются специфические для сектора закон и положение и не применяется значительный конкретный для сектора риск	Шкала реализации СМИБ Законы и руководящие документы (ИСО/МЭК 27001:2005, А.15)

На основе использования различных факторов из таблицы А.1 аспекты сложности области действия СМИБ могут классифицироваться по трем категориям: «высокая», «средняя» и «низкая». За общую категорию сложности может быть принята максимальная категория всех рассматриваемых факторов.

А.2 Специфические для сектора категории риска информационной безопасности

Риски для информации могут быть специфическими для вида рассматриваемой информации или сектора, в котором функционирует организация-клиент. Следующие примеры иллюстрируют различные категории риска.

Специфические категории, применяемые ко всем организациям-клиентам:

зарплаты, пенсии, здоровье и безопасность, документы организации-клиента, внутренняя и межведомственная информация, и т.д.;

любая другая лично идентифицируемая информация;

любая другая коммерчески секретная/важная информация, такая как научно-исследовательская, опытно-конструкторская, подробности об организации-клиенте, финансовые результаты и прогнозы, бизнес-планы, права на интеллектуальную собственность, производственные процессы и т.д.

Правительственная секретная/важная информация:

для общественности;

для электронного правительства;

о гражданах (например, здоровье, доходы, налоги, документы и т.д.);

которой оперируют правительственные поставщики и производители, такая как проекты ИКТ, оборудование, продукты, услуги и т.д.

Специфические категории, применяемые к классам организации:

корпоративное управление — перечисленные компании (возможно, также другие крупные экономические объекты).

Специфические категории, применяемые к секторам торгово-промышленной деятельности:

здравоохранение;

образование;

авиакосмическая промышленность;

телекоммуникации;

финансовые услуги;

благотворительные учреждения и некоммерческие организации.

Приложение В
(справочное)

Примерные области компетентности аудитора

В.1 Общая оценка компетентности

Существует несколько способов, с помощью которых аудитор может продемонстрировать свои знания и опыт, например, посредством использования общепризнанных квалификаций, регистрации под IRCA или любой другой признанной формы регистрации аудитора. Требуемый уровень компетентности для аудиторской группы должен быть установлен, согласуясь с промышленной/технологической областью организации и фактором сложности.

В.2 Специфическая оценка компетентности

В.2.1 Знание мер управления из приложения А ИСО/МЭК 27001:2005

Ниже изложены типовые вопросы проведения аудита СМИБ. Кроме знания мер управления из приложения А ИСО/МЭК 27001:2005, которые перечислены ниже, аудиторы должны быть осведомлены о других стандартах из серии ИСО/МЭК 27000.

Таблица В.1 — Меры управления

Типовые вопросы аудита	Источники, определяющие меры управления
Знание и опыт в политиках и требованиях деловой деятельности к информационной безопасности	Политика безопасности
Общее знание и опыт в бизнес-процессах, практиках и организационных структурах	Организация информационной безопасности
Знание оценки активов, материально-производственных запасов, классификаций и приемлемого использования политик	Управление активами
Общее знание и опыт в процессах и процедурах, используемых департаментами трудовых ресурсов	Безопасность трудовых ресурсов
Знание физической безопасности окружающей среды	Физическая безопасность и безопасность окружающей среды
Знание новейших стандартов, процессов, техник и методов, использованных для информационной безопасности, включая мероприятия менеджмента, а также наличие соответствующего уровня и опыта проведения технической экспертизы. Это включает в себя современные знания некоторых общих практик бизнеса	Управление коммуникациями и операциями Управление доступом Приобретение, разработка и обслуживание информационных систем
Современные знания и опыт в процессах и процедурах менеджмента инцидентов	Менеджмент инцидентов информационной безопасности
Современные знания и опыт в стандартах, процессах, планах и методах испытаний непрерывности бизнеса	Управление непрерывностью бизнеса
Современное знание вопросов контрактов бизнеса и общих законов и положений, связанных со СМИБ	Соответствие

В.2.2 Типичные знания, связанные с системой менеджмента информационной безопасности

Аудиторы должны знать и понимать следующие процессы проведения аудита и объекты СМИБ:

программирование и планирование аудита СМИБ;

тип и методология аудита СМИБ;

аудиторский риск;

анализ процессов информационной безопасности;

цикл Деминга (PDCA) для постоянного совершенствования;

проведение внутреннего аудита информационной безопасности.
Аудиторы должны знать и понимать следующие регулятивные требования:
интеллектуальная собственность;
содержание, защита и сохранение документов организации-клиента;
защита данных и конфиденциальность;
регулирование криптографических средств контроля;
предупреждение терроризма;
электронная коммерция;
электронные и цифровые подписи;
инспекция рабочих мест;
перехват в телекоммуникациях и мониторинг данных (например, электронная почта);
злоупотребление компьютером;
сбор электронных данных;
испытание на проникновение;
международные и национальные, конкретные для сектора, требования (например, банковское дело).
Аудиторы должны знать и понимать следующие требования менеджмента:
обработка рисков информационной безопасности;
риски безопасности аутсорсинга ICT;
риски информационной безопасности для цепочки поставок.

Приложение С
(справочное)

Продолжительность аудита

С.1 Введение

В настоящем приложении содержится дополнительная информация, касающаяся пунктов 9.1, 9.2, 9.3 и 9.4 ИСО/МЭК 17021:2006. Ее следует читать вместе с пунктами ИБ 9.1.2, ИБ 9.1.3, ИБ 9.1.5, ИБ 9.1.6, ИБ 9.2.3.1, ИБ 9.2.3.2 и ИБ 9.2.3.3 настоящего стандарта. Это приложение представляет собой руководство для органа сертификации по разработке собственных процедур определения времени, требуемого для сертификации области действия СМИБ организаций-клиентов различных размеров и сложности в широком спектре деятельности.

Органам сертификации необходимо определить продолжительность аудита, которая должна затрачиваться на первоначальную сертификацию, надзор и повторную сертификацию для каждой организации-клиента и сертифицированной СМИБ. Использование данного приложения в период планирования аудита может привести к формированию последовательного подхода к определению соответствующего времени, требуемого аудитору. В руководстве, приведенном в настоящем приложении, также учитываются гибкость в отношении результатов аудита, особенно во время его первого этапа, и сложность рассматриваемой области действия СМИБ.

С.2 Процедура определения продолжительности аудита

Опыт показывает, что область действия СМИБ и количество сотрудников (как проиллюстрировано в таблице времени аудитора в пункте С.3), размер, характеристики, сложность и значимость потенциальных рисков информационной безопасности (ниже объясняется более подробно) обусловливают время для аудитов данной СМИБ. В пункте ИБ 9.1.3, а также в пунктах ИБ 9.2.3.1, ИБ 9.2.3.2 и ИБ 9.2.3.3 перечисляются критерии, которые должны учитываться при определении необходимого времени аудитора. Эти и другие факторы должны рассматриваться в процессе анализа договора органа сертификации ввиду их потенциального влияния на назначение времени аудитора.

Важно отметить, что все эти факторы должны приниматься во внимание при определении продолжительности аудита и что таблица времени аудитора в пункте С.3 не может использоваться отдельно. Следующие примеры иллюстрируют факторы, которые могут повлиять на продолжительность аудита, и конкретизируют перечень факторов, данных в пункте ИБ 9.1.3, а именно:

факторы, касающиеся размера области действия СМИБ (например, количество использованных информационных систем, объем обрабатываемой информации, количество пользователей, количество привилегированных пользователей, количество платформ ИТ, количество объектов и их размер);

факторы, касающиеся сложности СМИБ (например, критичность информационных систем, ситуация риска СМИБ, объемы и виды обрабатываемой секретной и критической информации, количество и типы электронных сделок, количество и объем опытно-конструкторских работ, размер удаленного рабочего места, объем документации СМИБ);

вид(ы) деятельности, осуществляемой в области действия СМИБ, требования безопасности, правовые, регулирующие, договорные и требования, касающиеся этих видов деятельности;

объем и разнообразие технологий, использованных в реализации различных компонентов СМИБ (такие как: внедренные меры управления, контроль документации и/или управление процессом, корректирующие/предупредительные действия, информационные системы, системы ИТ, сети, например, являются ли они фиксированными, мобильными, беспроводными, внешними, внутренними);

количество объектов в пределах области действия СМИБ, насколько они идентичны или различны и будет ли проверяться вся совокупность объектов или выборка из них;

ранее продемонстрированное функционирование СМИБ;

объем аутсорсинга и мероприятий третьей стороны, использованных в области действия СМИБ и зависимость от этих услуг;

стандарты, законы и нормативы, применяющиеся к сертификации, и специфические для сектора требования, которые могут применяться.

Сертификация СМИБ обычно занимает больше времени, чем сертификация системы менеджмента качества или системы экологического менеджмента, из-за возросших требований к СМИБ, таких как требования к политике СМИБ, менеджменту риска, целям управления СМИБ и средствам контроля. Орган сертификации обязан:

a) проверить правильность и последовательность метода, посредством которого организация-клиент определяет значимость рисков информационной безопасности и воздействий на нее;

b) подтвердить, что система, предназначенная для достижения соответствия (со всеми соответствующими законами и другими требованиями, относящимися к СМИБ), способна это выполнить и что она работает и поддерживается;

c) подтвердить, что цели управления и средства контроля выбраны и реализованы правильно, их результативность оценивается и что процесс достижения «предотвращения и соответствующего реагирования на нарушения безопасности» является правильным и соблюдается;

d) подтвердить выполнение требований документации СМИБ организации-клиента;

e) реагировать на возросшие требования, появившиеся в результате первого этапа аудита.

С.3 Таблица времени аудитора

С.3.1 Общие положения

В таблице времени аудитора (таблица С.1) установлено среднее количество дней для первоначального аудита (здесь и в дальнейшем оно включает в себя дни аудита первого и второго этапов), которое, как показал опыт, целесообразно для области действия СМИБ с заданным числом сотрудников. Для областей действия сходных по размерам СМИБ требуется разное количество времени аудитора.

Изменение времени, затраченного на каждую сертификацию, зависит от количества факторов, включая размер, область действия аудита, материально-техническое обеспечение, сложность организации и ее состояние готовности к проведению аудита (см. также пункт С.2). Эти и другие факторы должны рассматриваться в процессе анализа договора органом сертификации ввиду их потенциального влияния на определение времени, требуемого аудитору. Следовательно, таблица времени аудитора не может использоваться отдельно.

Таблица времени аудитора представляет основную схему, которая может использоваться для планирования аудита путем определения отправной точки, основанной на общем количестве сотрудников всех смен, и регулирования этого количества на основе значимых факторов, применяющихся к области действия СМИБ, которая должна подвергаться аудиту, и придания каждому фактору своего коэффициента важности (аддитивный или субтрактивный) с целью определения необходимого числа сотрудников. Термины, использующиеся в этой таблице, объясняются в пункте С.3.2.

Таблица С.1 — Таблица времени аудитора

Количество сотрудников	Время аудитора для первоначального аудита системы менеджмента качества (дни аудитора)	Продолжительность первоначального аудита системы экологического менеджмента (дни аудитора)	Продолжительность первоначального аудита СМИБ (дни аудитора)	Аддитивные и субтрактивные факторы	Общее время аудитора
1~10	2	3	5	См. приложение С.2	
11~25	3		7	См. приложение С.2	
26~45	4	6	8,5	См. приложение С.2	
46~65	5		10	См. приложение С.2	
66~85	6		11	См. приложение С.2	
86~125	7	8	12	См. приложение С.2	
126~175	8		13	См. приложение С.2	
176~275	9		14	См. приложение С.2	
276~425	10		15	См. приложение С.2	
426~625	11	12	16,5	См. приложение С.2	
626~875	12		17,5	См. приложение С.2	
876~1,175	13		18,5	См. приложение С.2	
1,176~1,550	14		19,5	См. приложение С.2	
1,551~2,025	15	18	21	См. приложение С.2	
2,026~2,675	16		22	См. приложение С.2	
2,676~3,450	17		23	См. приложение С.2	
3,451~4,350	18		24	См. приложение С.2	
4,351~5,450	19		25	См. приложение С.2	
5,451~6,800	20		26	См. приложение С.2	
6,801~8,500	21		27	См. приложение С.2	
8,501~10,700	22		28	См. приложение С.2	
>10,700	Та же самая прогрессия		Та же самая прогрессия	См. приложение С.2	

С.3.2 Объяснение терминов

Термин «сотрудники», упоминающийся в таблице времени аудитора, относится ко всем лицам, чья рабочая деятельность имеет отношение к области действия СМИБ. Общее количество сотрудников всех смен является отправной точкой для определения продолжительности аудита.

Фактическое количество сотрудников включает непостоянный (сезонный, временный и субподрядный) штат, который будет представлен во время аудита. Орган сертификации должен согласовать с организациями-клиентами расчет продолжительности аудита, за которую наилучшим образом будет продемонстрирована вся область деятельности организации. По обстановке этот расчет может включать время года, месяц, день/дату и смену.

Частично занятые сотрудники должны рассматриваться как сотрудники с полной занятостью. Такое решение зависит от количества отработанных часов по сравнению с отработанными часами сотрудников с полной занятостью.

Термин «время аудитора» означает время, затраченное аудитором или аудиторской группой на первый и второй этапы аудита и планирование (включая при необходимости внешнюю проверку документов); согласование с организацией-клиентом, персоналом, записями, документацией и процессом; написание отчета. Предполагается, что «время аудитора», затраченное на планирование и написание отчета, обычно не должно сокращать общее «время аудитора» на месте менее чем до 70 % времени, показанного в таблице времени аудитора. Время передвижений аудитора не включается в этот расчет и является дополнительным ко времени аудитора, обозначенному в таблице.

Примечание 1 — 70 % времени являются фактором, основанным на опыте проведения аудитов СМИБ.

Если используются технологии проведения удаленного аудита, такие как интерактивное веб-сотрудничество, веб-собрания, телеконференции и/или электронная проверка процессов организации-клиента, они должны быть оговорены в плане аудита (см. ИБ 9.1.5) и могут рассматриваться как факторы, увеличивающие общее «время аудитора на месте».

Если орган сертификации разрабатывает план аудита, для которого технологии проведения удаленного аудита составляют более чем 30 % от запланированного времени аудитора на месте, орган сертификации должен обосновать этот план аудита и получить специальное одобрение от органа аккредитации до его реализации.

Примечание 2 — Время аудитора на месте относится ко времени аудитора, определенному для индивидуальных объектов. Электронные аудиты удаленных объектов рассматриваются как дистанционные аудиты, даже если эти электронные аудиты физически осуществляются в помещениях организации-клиента.

«Время аудитора» в таблице исчисляется в «днях аудитора», затраченных на аудит. Обычно «днем аудитора» является полный рабочий день.

Для цикла первоначального сертификационного аудита время надзора для данной организации должно быть пропорционально времени, затраченному на первоначальный аудит с общим временем, затраченным в год на надзор, составляющим 1/3 времени, затраченного на первоначальный аудит. Запланированное время надзора должно периодически пересматриваться, чтобы учесть все изменения в организации, технологическую зрелость системы и т.д., по крайней мере, во время аудита повторной сертификации.

Общее время, затраченное на осуществление аудита повторной сертификации, будет зависеть от полученных данных анализа, определенных в пункте ИБ 9.1.6 настоящего стандарта и ИСО/МЭК 17021:2006, пункт 9.4. Время, затраченное на повторный сертификационный аудит, должно быть пропорционально времени, затраченному на первоначальный сертификационный аудит той же самой организации, и должно составлять около 2/3 от времени, которое потребовалось бы для первоначального сертификационного аудита той же самой организации. Время аудита повторной сертификации превышает, как описано выше, время регулярного надзора, но когда повторный сертификационный аудит выполняется за то же самое время, что запланированная инспекция по регулярному надзору, аудита повторной сертификации также будет достаточно для удовлетворения требованиям к надзору. Руководство ИБ 9.1.2 применяется независимо от сделанного вывода.

После выбора общей отправной точки для определения необходимой продолжительности аудита области действия типичной СМИБ с заданным количеством сотрудников должны быть рассмотрены некоторые уточнения, чтобы учесть различия, которые могли бы повлиять на действительное время аудитора, необходимое для выполнения эффективного аудита для конкретной проверяемой СМИБ в дополнение к факторам, указанным в пункте С.2.

Примерными факторами, требующими дополнительного времени аудитора, могут быть:

сложное материально-техническое обеспечение, включающее более одного здания или помещения в области действия СМИБ;

штат, говорящий на нескольких языках (требуется переводчик (и) или предотвращение независимой работы отдельных аудиторов);

высокая степень регулирования;

СМИБ охватывает очень сложные процессы или относительно большое количество видов деятельности, или уникальную в своем роде деятельность;

процедуры, предусматривающие использование комбинации аппаратных средств, программного обеспечения процессов и услуг;

действия, требующие инспекции временных объектов для подтверждения правильности действия постоянного объекта(ов), чья система менеджмента подлежит сертификации (см. Примечание 3).

Примерными факторами, позволяющими сокращать время аудитора, могут быть:

процессы/продукты с низкой степенью риска;

априорное знание организации-клиента (например, если организация-клиент уже сертифицировалась по другому стандарту тем же органом сертификации);

готовность организации-клиента к сертификации (например, уже сертифицированной или признанной по другой схеме третьей стороны);

процессы, использующие один общий вид деятельности (например, только предоставление услуг);

зрелость системы менеджмента;

высокий процент сотрудников, выполняющих аналогичные простые задачи.

Примечание 3 — В ситуациях, когда клиент сертификации или сертифицированная организация представляет свой(и) продукт(ы) или услуги на временных объектах, важно, чтобы оценки подобных объектов включались в сертификационный аудит и программы надзора.

Временный объект — это место, отличное от объекта/места, идентифицированного в документе по сертификации, где деятельность в рамках области действия сертификации реализуется за определенный период времени. Эти объекты могут варьироваться от главных объектов по управлению проектом до второстепенных объектов для обслуживания/инсталляции. Необходимость инспекции подобных объектов и объем выборки объектов для проверки должны основываться на оценке рисков дефекта продукта или эксплуатационного отказа системы. Образец выбранных объектов должен представлять совокупность потребностей в компетентности и вариантов услуг организации-клиента с учетом масштабов и типов деятельности и различных этапов действующих проектов.

Необходимо рассматривать все особенности области действия СМИБ, процессы и продукты/услуги и осуществлять качественную корректировку факторов, которые могли бы более или менее обосновать время аудитора, требуемое для проведения эффективного аудита. Во всех случаях внесения поправок в таблицу времени аудитора для обоснования этих изменений .должно быть достаточно оснований и документов.

Приведенная диаграмма на рисунке С.1 иллюстрирует потенциальное влияние аддитивных и субтрактивных факторов на время, требуемое аудитору, из таблицы С.1.



Рисунок С.1 — Потенциальное влияние аддитивных и субтрактивных факторов на время, требуемое аудитору

Приложение D
(справочное)

Руководство по анализу реализованных мер управления из приложения А ИСО/МЭК 27001:2005

D.1 Цель

В настоящем приложении представлено руководство по анализу внедрения мер управления, перечисленных в приложении А ИСО/МЭК 27001:2005, и сбору свидетельств аудита в отношении эффективности этих мер во время первоначального аудита и последующих инспекций с целью надзора. Внедрение всех средств контроля, выбранных организацией-клиентом для СМИБ (согласно утверждению о применимости), должно проверяться во время второго этапа первоначального аудита и во время деятельности, связанной с надзором или повторной сертификацией.

Свидетельство аудита, которое собирает орган сертификации, должно быть достаточным, чтобы сделать вывод об эффективности мер управления. Каким образом предполагается осуществлять управление, должно быть определено в процедурах или политиках организации-клиента, заданных или взятых из утверждения о применимости. Очевидно, что меры управления вне области действия СМИБ проверяться не будут.

D.1.1 Свидетельство аудита

Наилучшее свидетельство аудита может быть получено в процессе визуального наблюдения аудитора (например, что запираемая дверь действительно заперта; что служащие действительно подписывают соглашения о соблюдении конфиденциальности; что перечень активов существует и содержит зарегистрированные активы; что находящиеся под наблюдением параметры настройки являются адекватными и т.д.). Свидетельство может быть получено на основе просмотра результатов осуществления контроля (например, распечаток прав доступа, подписанных соответствующим уполномоченным лицом; записей о разрешении инцидентов; полномочий для обработки, подписанных соответствующим уполномоченным лицом; протоколов административных (или других) совещаний и т.д.). Свидетельство может быть результатом прямого испытания аудитором (или повторного действия) средств контроля (например, попытки выполнить задачи, заявленные как запрещенные средствами контроля; определение, установлено ли программное обеспечение для защиты от вредоносной программы и обновляется ли оно на машинах, предоставляются ли права доступа (после проверки полномочий) и т.д.). Свидетельства могут собираться посредством проведения опроса сотрудников/подрядчиков о процессах и средствах контроля и определения, являются ли они действительно корректными.

D.2 Как работать с таблицей D.1

D.2.1 Колонки «Организационный контроль» и «Технический контроль»

«X» в соответствующей колонке показывает, является ли контроль организационным или техническим. Так как некоторые средства контроля являются как организационными, так и техническими, для таких средств контроля ставятся отметки в обеих колонках.

Свидетельства функционирования организационных средств контроля могут собираться при помощи анализа записей о функционировании средств контроля, опросов, наблюдения и физического осмотра. Свидетельства функционирования технических средств контроля зачастую могут собираться при помощи испытания системы или посредством использования специальных инструментов аудита/ предоставления отчетности.

D.2.2 Колонка «Испытание системы»

«Испытание системы» означает прямую проверку систем (например, проверка параметров настройки системы или конфигурации). Ответы на вопросы аудиторов можно получить на пульте управления системы, или они могут содержаться в оценке результатов тестирования инструментальных средств. Если организация-клиент имеет компьютерное инструментальное средство, известное аудитору, то оно может использоваться для поддержки аудита или для проверки результатов оценки, осуществленной организацией-клиентом (или ее субподрядчиками).

Существуют две категории проверки технических средств контроля:

«возможно»: тестирование системы возможно для оценки введения в действие средства контроля, но обычно это не является необходимым;

«рекомендуется»: тестирование системы обычно необходимо.

D.2.3 Колонка «Визуальная проверка»

«Визуальная проверка» означает, что обычно средства контроля для оценки их эффективности требуют визуального осмотра на месте. Это значит, что недостаточно проверить соответствующую документацию на бумаге или при помощи опросов — аудитор должен проверить это средство контроля на месте его эксплуатации.

D.2.4 Колонка «Руководство по анализу аудита»

В колонке «Руководство по анализу аудита» представлены возможные области повышенного внимания для оценки классифицируемой меры управления в качестве дальнейшего руководства для аудитора.

Таблица D.1 — Классификация мер управления

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.5 Политика безопасности					
А.5.1 Политика информационной безопасности (ИБ)					
А.5.1.1 Документация политики ИБ	X				
А.5.1.2 Анализ политики ИБ	X				Протоколы анализа со стороны руководства
А.6 Организация ИБ					
А.6.1 Внутренняя организация					
А.6.1.1 Обязательство менеджмента по ИБ	X				Протоколы заседаний руководства
А.6.1.2 Координация ИБ	X				Протоколы заседаний руководства
А.6.1.3 Распределение обязанностей по ИБ	X				
А.6.1.4 Процесс санкционирования средств обработки информации	X				
А.6.1.5 Соглашения о конфиденциальности	X				Выбрать несколько копий из архива
А.6.1.6 Контакт с властями	X				
А.6.1.7 Контакт со специальными группами людей, объединенными общими интересами	X				
А.6.1.8 Независимая проверка ИБ	X				Читать отчеты
А.6.2 Внешние стороны					
А.6.2.1 Определение рисков, связанных с внешними сторонами	X				
А.6.2.2 Определение безопасности при обращении с клиентами	X				
А.6.2.3 Определение безопасности в соглашениях с третьей стороной	X				Проверить некоторые условия контракта
А.7 Менеджмент активами					
А.7.1 Ответственность за активы					
А.7.1.1 Опись активов	X				Идентифицировать активы
А.7.1.2 Владение активами	X				
А.7.1.3 Приемлемое использование активов	X				

Продолжение таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.7.2 Классификация информации					
А.7.2.1 Правила классификации	X				
А.7.2.2 Маркировка и обработка информации	X				Наименование: директории, файлы, напечатанные отчеты, носители данных с записями (например, магнитные ленты, дискеты и CD), электронные сообщения и передача файлов
А.8 Кадровая безопасность					Провести выборку нескольких кадровых дел
А.8.1 Условия, предшествующие найму					
А.8.1.1 Роли и обязанности	X				
А.8.1.2 Отбор	X				
А.8.1.3 Условия найма	X				
А.8.2 Условия работы					
А.8.2.1 Обязанности руководства	X				
А.8.2.2 Осведомленность об ИБ, образование и обучение	X				Опросить штат, осведомлены ли они о конкретных вопросах, которые они должны знать
А.8.2.3 Процесс, связанный с дисциплиной	X				
А.8.3 Окончание или изменение работы по найму					
А.8.3.1 Обязанности, связанные с окончанием найма	X				
А.8.3.2 Возвращение активов	X				
А.8.3.3 Лишение прав доступа	X	X	Рекомендуется		
А.9 Физическая защита от влияния окружающей среды					
А.9.1 Безопасные области					
А.9.1.1 Периметр физической защиты	X				
А.9.1.2 Средства физического контроля входа в помещение	X	X	Возможно	X	Архивирование записей о доступе
А.9.1.3 Обеспечение безопасности офисов, комнат и помещений	X			X	
А.9.1.4 Защита от внешних угроз и угроз окружающей среды	X			X	

Продолжение таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.9.1.5 Работа в безопасных зонах	X			X	
А.9.1.6 Области доступа к местам общественного пользования, поставки и погрузки	X			X	
А.9.2 Безопасность оборудования					
А.9.2.1 Размещение оборудования и его защита	X	X	Возможно	X	
А.9.2.2 Вспомогательное оборудование	X	X	Возможно	X	
А.9.2.3 Безопасность кабельной системы	X			X	
А.9.2.4 Обслуживание оборудования	X				
А.9.2.5 Безопасность дистанционного оборудования	X	X	Возможно		Шифрование портативных (переносных) устройств
А.9.2.6 Безопасное устранение или повторное использование оборудования	X	X	Возможно	X	
А.9.2.7 Ликвидация собственности	X				
А.10 Управление коммуникациями и их работой					
А.10.1 Эксплуатационные процедуры и обязанности					
А.10.1.1 Документально оформленные способы эксплуатации	X				
А.10.1.2 Управление изменениями	X	X	Рекомендуется		
А.10.1.3 Распределение обязанностей	X				
А.10.1.4 Разделение разработки, испытания и рабочего оборудования	X	X	Возможно		
А.10.2 Управление доставкой услуг третьей стороной					
А.10.2.1 Доставка услуг	X				
А.10.2.2 Мониторинг и проверка услуг третьей стороны	X	X	Возможно		
А.10.2.3 Менеджмент изменениями услуг третьей стороны	X				
А.10.3 Планирование и приемка системы					

Продолжение таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.10.3.1 Управление пропускной способностью	X	X	Возможно		
А.10.3.2 Приемка системы	X				
А.10.4 Защита от вредоносного программного обеспечения и мобильных программ					
А.10.4.1 Средства контроля в отношении вредоносного программного обеспечения	X	X	Рекомендуется		Выборка серверов, настольных компьютеров, межсетевых интерфейсов
А.10.4.2 Средства контроля в отношении мобильных программ	X	X	Возможно		
А.10.5 Резервирование					
А.10.5.1 Резервирование информации	X	X	Рекомендуется		Попытаться восстановить
А.10.6 Управление защитой сети					
А.10.6.1 Средства контроля сети	X	X	Возможно		
А.10.6.2 Безопасность сетевых услуг	X				Соглашения об уровне сервиса, функции безопасности
А.10.7 Обращение с носителями информации					
А.10.7.1 Управление съемными носителями информации	X	X	Возможно		
А.10.7.2 Уничтожение носителей информации	X				
А.10.7.3 Процедуры обработки информации	X				
А.10.7.4 Безопасность документации системы	X	X	Возможно	X	
А.10.8 Обмен информацией					
А.10.8.1 Политики и процедуры обмена информацией	X				
А.10.8.2 Соглашения об обмене	X				
А.10.8.3 Физические носители информации в процессе передачи	X	X	Возможно		Шифрование или физическая защита
А.10.8.4 Электронный обмен сообщениями	X	X	Возможно		Подтвердить, что выборочные сообщения соответствуют политике/процедурам
А.10.8.5 Системы бизнес-информации	X				
А.10.9 Услуги электронной коммерции					

Продолжение таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.10.9.1 Электронная коммерция	X	X	Возможно		
А.10.9.2 Сделки в режиме он-лайн	X	X	Рекомендуется		Проверить: целостность, авторизацию доступа
А.10.9.3 Общедоступная информация	X	X	Возможно		
А.10.10 Мониторинг					
А.10.10.1 Ведение регистрации аудита	X	X	Возможно		Он-лайн или печатная
А.10.10.2 Мониторинг использования системы	X	X	Возможно		
А.10.10.3 Защита информации журналов регистрации	X	X	Возможно		
А.10.10.4 Журналы регистрации деятельности администраторов и операторов	X	X	Возможно		
А.10.10.5 Фиксирование ошибок	X				
А.10.10.6 Синхронизация часов		X	Возможно		
А.11 Контроль доступа					
А.11.1 Требования бизнеса к контролю доступа					
А.11.1.1 Политика контроля доступа	X				
А.11.2 Управление доступом пользователей					
А.11.2.1 Регистрация пользователей	X				Выбрать сотрудников/подрядчиков для проверки наличия разрешений всех прав доступа ко всем системам
А.11.2.2 Управление привилегиями	X	X	Возможно		Внутреннее перемещение штата
А.11.2.3 Управление паролями пользователей	X				
А.11.2.4 Пересмотр прав доступа пользователей	X				
А.11.3 Обязанности пользователей					
А.11.3.1 Использование паролей	X				Проверить руководства/политику для пользователей
А.11.3.2 Оборудование, не обслуживаемое пользователем	X				Проверить руководства/политику для пользователей
А.11.3.3 Политика чистого рабочего стола и чистого экрана	X			X	

Продолжение таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.11.4 Контроль доступа к сети					
А.11.4.1 Политика использования сетевых услуг	X				
А.11.4.2 Аутентификация пользователя для внешних соединений	X	X	Рекомендуется		
А.11.4.3 Идентификация оборудования сетей		X			
А.11.4.4 Защита дистанционной диагностики и порта конфигурации		X	Рекомендуется		
А.11.4.5 Разделение в сетях	X	X	Возможно		Сетевые графики: глобальная сеть, локальная сеть, виртуальная локальная сеть, виртуальная частная сеть, сетевые объекты, сегменты сети (например, демилитаризованная зона)
А.11.4.6 Контроль сетевых соединений	X	X	Рекомендуется		Совместно используемые сети, мало распространенные сети
А.11.4.7 Контроль маршрутизации в сети	X	X	Рекомендуется		Межсетевые экраны, маршрутизаторы/переключатели: база правил, списки управления доступом, политики управления доступом
А.11.5 Контроль доступа к операционным системам					
А.11.5.1 Процедуры безопасного входа в систему	X	X	Рекомендуется		
А.11.5.2 Идентификация и аутентификация пользователей	X	X	Рекомендуется		
А.11.5.3 Система управления паролями	X	X	Рекомендуется		
А.11.5.4 Использование системных утилит	X	X	Рекомендуется		
А.11.5.5 Лимит времени в сеансе связи	X	X	Возможно	X	
А.11.5.6 Ограничение времени соединения	X	X	Возможно	X	
А.11.6 Управление доступом к информации					
А.11.6.1 Ограничение доступа к информации	X	X	Рекомендуется		
А.11.6.2 Изоляция секретной системы	X	X	Возможно		

Продолжение таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.11.7 Мобильные компьютерные среды и дистанционная работа					
А.11.7.1 Мобильные компьютерные среды и коммуникации	X	X	Возможно		
А.11.7.2 Дистанционная работа	X	X	Возможно		
А.12 Приобретение, разработка и обслуживание информационных систем					
А.12.1 Требования безопасности информационных систем					
А.12.1.1 Анализ и подробное изложение требований безопасности	X				
А.12.2 Правильная обработка данных в прикладных программах					
А.12.2.1 Подтверждение правильности входных данных	X	X	Рекомендуется		Руководства по разработке программного обеспечения, тестирование программных средств; подтвердить в выборке бизнес-приложений, что средства контроля, требующиеся пользователям, существуют на практике
А.12.2.2 Управление внутренней обработкой	X	X	Возможно		Принципы разработки программных средств, тестирование программных средств; подтвердить в выборке бизнес-приложений, что требующиеся пользователям средства контроля существуют на практике
А.12.2.3 Целостность сообщений		X	Возможно		
А.12.2.4 Подтверждение правильности выходных данных	X	X	Возможно		Руководства по разработке программного обеспечения, тестирование программных средств; подтвердить в выборке бизнес-приложений, что средства контроля, требующиеся пользователям, существуют на практике
А.12.3 Криптографические средства контроля					
А.12.3.1 Политика использования криптографических средств контроля	X	X	Возможно		Проверить также внедрение политики, где это необходимо
А.12.3.2 Распределение ключей	X	X	Рекомендуется		

Продолжение таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.12.4 Безопасность системных файлов					
А.12.4.1 Контроль системного программного обеспечения	X	X	Возможно		
А.12.4.2 Защита данных испытаний системы	X	X	Возможно	X	
А.12.4.3 Контроль доступа к коду источника программы	X	X	Рекомендуется		
А.12.5 Обеспечение безопасности в процессах разработки и поддержки					
А.12.5.1 Процедуры контроля изменений	X				
А.12.5.2 Техническая проверка приложений после изменений в операционной системе	X				
А.12.5.3 Ограничения по изменениям в программных пакетах	X				
А.12.5.4 Утечка информации	X	X	Возможно		Неизвестные услуги
А.12.5.5 Разработка программного обеспечения аутсорсинга	X				
А.12.6 Управление технической уязвимостью					
А.12.6.1 Контроль технических уязвимостей	X	X	Рекомендуется		Распределение патчей
А.13 Менеджмент инцидентов информационной безопасности					
А.13.1 Составление отчетов о событиях, связанных с ИБ, и слабых местах					
А.13.1.1 Составление отчетов о событиях, связанных с ИБ	X				
А.13.1.2 Составление отчетов о слабых местах безопасности	X				
А.13.2 Менеджмент инцидентов ИБ и улучшений					
А.13.2.1 Обязанности и процедуры	X				
А.13.2.2 Извлечение уроков из инцидентов ИБ	X				
А.13.2.3 Сбор данных	X				

Продолжение таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.14 Управление непрерывностью бизнеса					
А.14.1 Аспекты ИБ управления непрерывностью бизнеса					Протоколы анализа со стороны руководства
А.14.1.1 Включение безопасности в процесс управления непрерывностью бизнеса	X				
А.14.1.2 Обеспечение непрерывности бизнеса и оценка риска	X				
А.14.1.3 Разработка и реализация планов непрерывности бизнеса, включая ИБ	X	X	Возможно	X	Инспекция объектов для восстановления после бедствия, удаленность объектов для восстановления после бедствия в соответствии с оценкой риска и применимыми правовыми/регулирующими требованиями
А.14.1.4 Основа планирования непрерывности бизнеса	X				
А.14.1.5 Тестирование поддержания и повторной оценки планов непрерывности бизнеса	X				
А.15 Соответствие					
А.15.1 Соответствие правовым требованиям					
А.15.1.1 Определение применимого законодательства	X				
А.15.1.2 Права на интеллектуальную собственность	X				
А.15.1.3 Защита документов организации	X	X	Возможно		
А.15.1.4 Защита данных и обеспечение конфиденциальности личной информации	X	X	Возможно		
А.15.1.5 Предотвращение неправильного использования средств обработки информации	X				
А.15.1.6 Регулирование криптографических средств контроля	X				
А.15.2 Соответствие политикам и стандартам безопасности и техническое соответствие					
А.15.2.1 Соответствие политикам и стандартам безопасности	X				

Окончание таблицы D.1

Меры управления в приложении А ИСО/МЭК 27001:2005	Организационный контроль	Технический контроль	Испытание системы	Визуальная проверка	Руководство по анализу аудита
А.15.2.2 Проверка технического соответствия	X	X			Оценить процесс и дополнительные данные
А.15.3 Рассмотрение аудита информационных систем					
А.15.3.1 Средства контроля аудита информационных систем	X				
А.15.3.2 Защита инструментальных средств аудита информационных систем	X	X	Возможно		

Приложение Е
(обязательное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица Е.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 9000:2005	IDT	ГОСТ Р ИСО 9000—2008 Системы менеджмента качества. Основные положения и словарь
ИСО 9001:2008	IDT	ГОСТ Р ИСО 9001—2008 Системы менеджмента качества. Требования
ИСО/МЭК 17021:2006	IDT	ГОСТ Р ИСО/МЭК 17021—2008 Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента
ИСО 19011:2002	IDT	ГОСТ Р ИСО 19011—2003 Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

УДК 351.864.1:004:006.354 ОКС 35.040 ТО

Ключевые слова: сертификация, аудит, орган сертификации, система менеджмента информационной безопасности

Редактор *Н.В. Авилочкина*
Технический редактор *Н.С. Гришанова*
Корректор *Р.А. Ментова*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 31.05.2010. Подписано в печать 21.06.2010. Формат 60x84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 4,65. Уч.-изд. л. 4,85. Тираж 180 экз. Зак. 506.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru